REMARKS

Applicant wishes to thank the Examiner for the thoughtful examination. In view of the amendments and the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application.

Amendments

Independent claims 1, 9, 16, 23 and 30 are amended herein. Support for these claim amendments can be found in the original disclosure at least at paragraphs [0043] on page 11, lines 11-21 and [0039] on page 10, lines 11-15.

Dependent claims 10-13 and 15 have been amended to be consistent with amended claim 9 upon which they depend.

Claim 23 is amended to address the Examiner's objection. Support for this amendment can be found in the original disclosure at least at paragraph [0017] on page 4, lines 14-17

Claims 6 and 14 are canceled and their elements incorporated into claims 1 and 9 respectively.

Rejection of Claim 29 under § 112 ¶ 2

Claim 29 was rejected under 35 U.S.C. § 112, ¶ 2. Without conceding the propriety of the rejection, and in the interest of expediting allowance of the application, claim 23 from which claim 29 depends, is amended.

Rejection of Claims 9-34 under 35 U.S.C. § 101

Claims 9-34 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Without conceding the propriety of the rejection, and in the interest of expediting allowance of the application, independent claims 9, 16, 23 and 30 are amended for clarification. Dependent claims have been amended to maintain consistency with the independent claims from which they depend.

Rejection under 35 U.S.C. § 103(a)

Claims 1-3, 6-11, 14-19, 22, 30, 31, and 34 stand rejected under 35 U.S.C. § 103(a) as being obvious over Enhanced IP Services for Cisco Networks ("Cisco") in view of C.O.B.A.S. Centralized Out-of-Band Authentication System ("COBAS"). Applicant respectfully traverses this rejection. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claims 1, 9-13, 15, 16, 23, 30, and 34 have been amended as proposed during the interview and are believed to be allowable.

Claim 1 is an independent claim which, as amended, recites:

An out-of-band method for asynchronously establishing a trust

relationship with a remote node, comprising:
generating a local public value and a local private value on at least one node;
storing the public value on an out-of-band computer-readable medium;
transporting the out-of-band computer-readable medium to the other node;
receiving the public value from the other node via the out-of-band computer-readable medium; and
generating a secret value using the local private value in combination with the public value received from the other node; wherein the receiving is asynchronous to the generating.

The Examiner has failed to establish a prima facie case of obviousness for at least these three reasons:

- The combination fails to teach or suggest all of the elements claimed. COBAS only teaches the out-of-band transmission of user authentication information via a separate network for an existing link and fails to teach "transporting the out-of-band computer-readable medium to the other node; receiving the public value from the other node via the out-of-band computer-readable medium; and generating a secret value using the local private value in combination with the public value received from the other node; wherein the receiving is asynchronous to the generating."
- The combination renders both Cisco and COBAS unsatisfactory for their intended purposes.
- Both Cisco and COBAS teach away from implementing this modification, resulting in a lack of motivation to combine.

Cisco is cited for its teaching of establishing a trust relationship with a remote node. The Examiner recognizes, however, that Cisco fails to teach out-of-band transmission (Office Action, page 5), and cites COBAS merely to show out-of-band transmission generally. COBAS only teaches the real-time out-of-band transmission of user authentication information via a separate communications network for providing access to an existing connection. (COBAS, page 5) Therefore COBAS

fails to teach or disclose "transporting the out-of-band computer-readable medium to the other node; receiving the public value from the other node via the out-of-band computer-readable medium; and generating a secret value using the local private value in combination with the public value received from the other node; wherein the receiving is asynchronous to the generating."

Authentication differs from the transporting of public values, such as the exchange of key data necessary to setup an encrypted connection. To create a functioning encrypted connection, an exchange of encryption keys must occur at some point. That exchange may occur without authentication, and indeed commonly occurs without authentication in the case of public key/private key pairs where the public key is distributed without restriction. (Office Action, p12 citing PGP) The user may then optionally be required to verify their identity, or authenticate, via a user name and password to enable passage of traffic along the connection or access specific resources. Thus, authentication and key exchange are not the same.

COBAS teaches the real-time out-of-band transmission of user authentication information via a separate communications network for providing access to an existing connection. (COBAS, page 5) While the user authentication information is transmitted out-of-band (via a different network then that which the user is trying to access) the authentication step is occurring on demand between the end user and the authentication module to allow access, and is thus a synchronous communication. (COBAS, pages 6, 8)

COBAS therefore teaches synchronous generation followed by immediate receipt of authentication information, but fails to disclose or suggest that "the receiving is asynchronous to the generating" as presently recited in independent claim 1.

Moreover, as COBAS is direct to the transmission of authentication information, it fails to disclose or suggest "storing the public value on an out-of-band computer-readable medium" or "transporting the out-of-band computer-readable medium," as presently recited in independent claim 1.

Finally, where COBAS involves a separate network for transmitting authentication information, applicant is "transporting the out-of-band computer-readable medium" which contains "the public value."

As Cisco and COBAS, whether taken alone or in combination fail to teach or suggest the features recited in claim 1, it is respectfully submitted that the claim is allowable over the cited prior art.

The proposed combination renders Cisco and COBAS unsatisfactory for their intended purposes

Combining Cisco and COBAS as proposed by the Examiner would render the references unsatisfactory for their intended purpose. "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)"

MPEP § 2143.01(V). Cisco seeks to eliminate out-of-band transmissions of encryption keys altogether and thus facilitate in-band exchanges. (Cisco, pages 2-3) COBAS is designed to use "a separate network" for authentication, not transmission of encryption keys. (COBAS, page 5). Given that Cisco uses in-band transmission of encryption keys to facilitate setup and COBAS only handles authentication data, such a combination would render both references unsatisfactory for their respective intended purposes: Cisco for now requiring a "cumbersome" (Cisco, page 3, line 2) out-of-band method and COBAS for handling unwieldy encryption keys rather than authentication info. Therefore, a prima facie case of obviousness has not been made and claim 1 should be allowed.

Lack of Motivation to Combine

Cisco teaches away from out-of-band transmission as being "cumbersome" (Cisco, page 3, line 2) and that it "does not scale to the size needed for large networks" (Cisco, page 3, lines 4-5), then proceeds to discuss in-band transmission of keys. The Examiner uses COBAS merely to teach out-of-band transmission generally. However, COBAS explicitly teaches away from the use of physical media by requiring "a separate network" for access to the authentication server. (COBAS, page 5)

In rejecting claim 8, the Examiner states that "It would have been obvious to one of ordinary skill in the art at the time of [sic] invention was made to incorporate the teachings of C.O.B.A.S. in to the teachings of Cisco, because one

of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks." (Emphasis Added) (Office Action, page 8) COBAS addresses authentication of the user, as distinguished from the exchange of encryption keys necessary to setup an encrypted connection. As the name "Centralized Out-Of-Band *Authentication* System" itself states, COBAS uses the out-of-band transmission only for authentication, (COBAS, pages 5, 7) not for exchange of encryption data to setup an encryption channel. As one of ordinary skill in the art can appreciate, authentication differs from the key exchange in an encrypted connection. For example, a user may have an encrypted connection back to the office, but is then required to authenticate via a user name and password to enable passage of traffic along the connection. Authentication without the presence of an encrypted link merely identifies a user without permitting access. More commonly, a user may have access to an encrypted connection but authentication is required to use resources available via that connection. COBAS addresses this issue by teaching an out of band authentication method in which a user communicates with the authentication server via a separate network and receives an authentication key. However, COBAS does not teach or suggest "storing the public value on an out-of-band computer-readable medium; transporting the out-of-band computer-readable medium to the other node," as recited in claim 1.

Since Cisco actively disparages out-of-band transmission of encryption keys and COBAS focuses only on real-time authentication via a separate network and not the exchange of key data, a person of ordinary skill in the art would not have combined them. Indeed, as discussed above, both inventions would be rendered unsatisfactory for their intended purposes by such a combination. Therefore Cisco and COBAS are not appropriate prior art and applicant's invention is patentably distinguishable.

The Examiner has rejected claim 7, citing Cisco in view of COBAS. **Claim 7** as presented recites:

> A method according to Claim 1, wherein the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device.

COBAS is directed to an out-of-band transmission of user authentication information, and teaches the exchange of one-time passwords through the use of special hardware devices ("tokens"). (COBAS, Page 4) COBAS teaches using a set of previously exchanged encryption key values to encode for secure transport a one-time password used for authentication. However, COBAS fails to disclose or suggest "generating a local public value and a local private value" as recited in claim 1 and "receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device" as recited in claim 7.

The Examiner states "It would have been obvious to one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such

as key exchanges from interception, unauthorized monitoring and man in the middle attacks." (Emphasis added) (Office Action, page 7) However, as stated above in response to the rejections of claims 1, COBAS only teaches the exchange of authentication data and not "receiving of [a] public value from [another] node via an out-of-band mechanism [the receiving including] downloading the public value from an external device" as recited in claim 7. Thus, claim 7 is in condition for allowance.

Claim 8 as presented recites:

> A method according to Claim 7, wherein the transporting external device is any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

The Examiner states "It would have been obvious to one of ordinary skill in the art would be motivated to protect or insulate authentication transactions such as key exchanges from interception, unauthorized monitoring and man in the middle attacks." (Emphasis added) (Office Action, page 8) However, as stated above in response to the rejections of claims 1 and 7, COBAS only teaches exchange of authentication data not encryption keys used to encode data. Neither reference teaches transporting encryption keys via an external device. Thus, for the reasons stated above in response to the rejections of claims 1 and 7, this claim is in condition for allowance.

Dependent claims 2-3 and claims 7-8 depend from claim 1 and are also allowable by virtue of their dependencies as well as for the additional features that they recite.

Claim 9 and its dependent claims 10-15 were rejected for the same reasons as set forth in claim 1 and its dependents. Claim 9 as amended recites:

> A computer-readable storage medium having one or more instructions causing one or more processors to:
> generate a local two-part code having a public code component and private code component;
> store the public component on a peripheral out-of-band device which is then transported to a another processor;
> receive the public code component asynchronously from another processor via the peripheral device; and
> generate a secret value using the local private code component and the public code component received from the other processor.

For the reasons stated above regarding claim 1, independent claim 9 which recites similar features is also allowable as are its dependent claims by virtue of their dependencies as well as for the additional features that they recite.

Claim 16 and its dependent claims 17-22 were rejected for the same reasons as set forth in claim 1 and its dependents. Claim 16 as amended recites:

> An apparatus, comprising:
> a computer-readable storage medium;
> a key generator on a first node to generate a local public/private key pair;
> a computer processor capable of writing the local

public/private key pair to an out-of-band computer-readable storage medium;

a method of transporting the out-of-band computer readable storage medium to a second node; and

a shared secret generator on the second node to receive the public key from the first another node via the out-of-band computer-readable storage medium connection and which is able to generate a shared secret using the local private key and the public key received from the first other node.

For the reasons stated above regarding claim 1, independent claim 16 which recites similar features is also allowable as are its dependent claims by virtue of their dependencies as well as for the additional features that they recite.

Claim 30 and its dependent claims 31-34 were rejected for the same reasons as set forth in claim 1 and its dependents. Claim 30 as amended recites:

An apparatus, comprising:

means for generating a local public/private key pair;

means for storing a public key on an out-of-band computer-readable medium;

means for transporting asynchronously the public key to another node;

means for receiving at another node the public key from the out-of-band computer-readable medium; and

means for generating a shared secret using the local private key and the public key received from the other node asynchronously via the out-of-band computer-readable medium.

For the reasons stated above regarding claim 1, independent claim 30 which recites similar features is also allowable as are its dependent claims by virtue of their dependencies as well as for the additional features that they recite.

Claims 1, 4-9, 12-16, 18, 20-22, 30, and 32-34 were rejected under 35 U.S.C. § 103(a) as being obvious over Cisco in view of COBAS and Pretty Good Privacy PGP for Personal Privacy, Version 5.0 ("PGP").

Applicant respectfully traverses this rejection. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claims 1, 9, 12-13, 15-16, 30, and 34 have been amended as proposed during the interview and are believed to be allowable.

As described above, COBAS and Cisco when combined fail to teach or suggest all of the elements claimed, in particular the out-of-band transmission of the keys necessary to setup an encrypted link. Even if all elements were taught, such a combination would render both Cisco and COBAS unsatisfactory for their intended purposes. Finally, both Cisco and COBAS teach away from implementing this modification, resulting in a lack of motivation to combine.

PGP is directed to an encryption system using public key encryption. PGP was cited for its teaching of establishing a trust relationship with a remote node, generating a local public value and a local private value on at least one node, and receiving a public value from another node. However, PGP fails to disclose or suggest "storing the public value on an out-of-band computer-readable medium" and "transporting the out-of-band computer-readable medium to the other node" as presently recited in claim 1. COBAS is cited to remedy this defect, but as

described above, COBAS relates to the exchange of authentication data, not encryption keys.

For the reasons stated above regarding claim 1, independent claims 9, 16, and 30 which recite similar features are also allowable as are their dependent claims by virtue of their dependencies as well as for the additional features that they recite.

Claims 23 and 27-29 were rejected under 35 U.S.C. § 103(a) as being obvious over PGP in view of COBAS.

Applicant respectfully traverses this rejection. Nevertheless, without conceding the propriety of the rejection and in the interest of expediting allowance of the application, claim 23 has been amended as proposed during the interview and is believed to be allowable.

Independent claim 23 as presented, recites:

> A protocol for establishing trust between two or more processing nodes, comprising:
> generating a public key and a private key on each of at least two nodes;
> exchanging the public keys asynchronously between the at least two nodes using an out-of-band mechanism comprising a computer-readable storage medium; and
> calculating a secret to be shared on at least one of the two nodes.

PGP is directed to an encryption system using public key encryption. However, PGP fails to disclose or suggest "exchanging the public keys asynchronously between the at least two nodes using an out-of-band mechanism

comprising a computer-readable storage medium," as presently recited in claim 23.

COBAS was cited for its alleged teaching of "using an asynchronous mechanism" (Office Action, page 21). However, as discussed above, COBAS teaches the real-time out-of-band transmission of user authentication information via a separate communications network for providing access to an existing connection. (COBAS, pages 5, 6, and 8) COBAS uses "asynchronous" to indicate the use of a separate real-time communications network. COBAS therefore actually teaches a temporally synchronous process of exchanging authentication information via a separate real-time (or nearly so) network. As such, COBAS teaches a synchronous authentication system and not "exchanging the public keys asynchronously between the at least two nodes using an out-of-band mechanism comprising a computer-readable storage medium" as presently recited in independent claim 23.

Thus, COBAS and PGP, whether taken alone or in combination (assuming for the sake of argument that they can be combined), fail to disclose or suggest the features of claim 23. Accordingly, as discussed during the interview, independent 23 is allowable.

The Examiner's rejections of dependent claims 27-29 incorporate the rejection of claim 23. However, as described above, all of the elements of claim 23 are not taught by the references. Since dependent claims 27-29 depend from independent claim 23, they are allowable by virtue of this dependency, as well as for additional features that they recite.

Claims 24-26 were rejected under 35 U.S.C. § 103(a) as being obvious over Cisco in view of COBAS and PGP.

The Examiner's rejections of dependent claims 24-26 incorporate the rejection of claim 23. However, as described above, all of the elements of claim 23 are not taught by the references. Since dependent claims 24-26 depend from independent claim 23, they are allowable by virtue of this dependency, as well as for additional features that they recite.

CONCLUSION

For at least the foregoing reasons, the claims are believed to be in condition for allowance.

If any issue remains unresolved that would prevent allowance of this case, **the Examiner is requested to contact the undersigned attorney to resolve the issue**.

Respectfully submitted,

Date: 10/24/2007

By: 

Christopher Lattin
Lee & Hayes, pllc
Reg. No. 56,064
(509) 324-9256 ext. 263